FPKIPA

Federal Public Key Infastructure Policy Authority

**Common Policy Change Proposal Number: 2006-02**

**To:** Federal PKI Policy Authority

**From:** Certificate Policy Working Group

**Subject:** Proposed modifications to the Common Certificate Policy

**Date:** 28 September 2006

**Title:** Accelerated adoption of changes in draft RFC 3647 version of policy

**Version and Date of Certificate Policy Requested to be changed:**

X.509 Certificate Policy for the Common Policy Framework Version 2.4, 15 February 2006.

**Change Advocate's Contact Information:**

Name: David Cooper
Organization: NIST
Telephone number: 301-975-3194
E-mail address: david.cooper@nist.gov

**Organization requesting change**: Federal PKI Policy Authority

**Change summary**: Federal agencies are required to begin issuing certificates in conformance with FIPS 201 beginning October 27, 2006. The changes incorporated in this change proposal are needed to aid agencies in satisfying that requirement.

**Background**: The draft RFC 3647 formatted version of the Common Policy includes a number of changes that were included to satisfy agency requirements and based on experience with the current policy. With the looming deadline to begin issuing PIV Authentication certificates, agencies cannot wait until the RFC 3647 formatted version of the Common Policy has been approved for these changes to be accepted.

## Issue

The draft RFC 3647 formatted version of the Common Policy includes slightly relaxed rules for the construction of subject names longer maximum lifetimes for certain certificates and key pairs. Agencies require these changes to the policy in order to accommodate organizational requirements and cannot wait until the RFC 3647 formatted version of the Common Policy has been approved. In addition, the Common Policy does not address the needs of CAs that issue short lifetime certificates to OCSP responders. This change proposal allows for certificates issued to OCSP responders to be renewed and allows CAs to use their private keys to sign OCSP responder certificates for the entire lifetime of the entire lifetime of the CA's key pair.

**Specific Changes:**

Specific changes are made to the sections 3.1.1, 3.2.1, 4.4.3, 4.7, and 6.3.2. Insertions are underlined, deletions are in ~~strikethrough~~.

### 3.1.1 Types of Names

For certificates issued under id-fpki-common-policy, id-fpki-common-hardware, id-fpki-common-High, and id-fpki-common-devices, the CA shall assign X.500 distinguished names to all subscribers. These distinguished names may be in either of two forms: an X.501 distinguished name specifying a geo-political name; or an Internet domain component name.

All geo-political X.501 distinguished names assigned to federal employees shall be in one of the following directory information trees:

C=US, o=U.S. Government, [ou=*department*], [ou=*agency*], [ou=*structural_container*]
C=US, [o=*department*], [ou=*agency*], [ou=*structural_container*]

New implementations shall assign names in the following directory tree:
C=US, o=U.S. Government, [ou=*department*], [ou=*agency*], [ou=*structural_container*]

The organizational units *department* and *agency* appear when applicable and are used to specify the federal entity that employs the subscriber. At least one organizational unit must appear in the DN. The additional organizational unit *structural_container* is permitted to support local directory requirements, such as differentiation between human subscribers and devices. This organizational unit may not be employed to further differentiate between subcomponents within an agency.

The distinguished name of the federal employee subscriber will take one of the three following forms:

- C=US, o=U.S. Government, [ou=*department*], [ou=*agency*], [ou=*structural_container*], cn=*nickname lastname*
- C=US, o=U.S. Government, [ou=*department*], [ou=*agency*], [ou=*structural_container*], cn=*firstname initial. lastname*
- C=US, o=U.S. Government, [ou=*department*], [ou=*agency*], [ou=*structural_container*], cn=*firstname middlename lastname*

In the first name form, *nickname* may be the subscriber's first name, a form of the first name, middle name, or pseudonym (e.g., Buck) by which the subscriber is generally known. A generational qualifier, such as "Sr." or "III", may be appended to any of the common name forms specified above.

X.501 distinguished names assigned to federal contractors and other affiliated persons shall be within the same directory information tree. The distinguished name of the federal contractor subscribers and affiliate subscribers will take one of the three following forms:

- C=US, o=U.S. Government, [ou=*department*], [ou=*agency*], [ou=*structural_container*], cn=*nickname lastname* (affiliate)
- C=US, o=U.S. Government, [ou=*department*], [ou=*agency*], [ou=*structural_container*], cn=*firstname initial. lastname* (affiliate)
- C=US, o=U.S. Government, [ou=*department*], [ou=*agency*], [ou=*structural_container*], cn=*firstname middlename lastname* (affiliate)

For names assigned to federal contractors and other affiliated persons, generational qualifiers may be inserted between *lastname* and "(affiliate)".

Legacy implementations which predate this policy may use the directory tree:
C=US, [o=*department*], [ou=*agency*], [ou=*structural_container*]
Common name fields shall be populated as specified above.

Distinguished names based on Internet domain component names shall be in the following directory information trees:

dc=gov, dc=*org0*, [dc=*org1*],…[ dc=*orgN*], [ou=*structural_container*]
dc=mil, dc=*org0*, [dc=*org1*],…[ dc=*orgN*], [ou=*structural_container*]

The default Internet domain name for the agency, [*orgN*.]…[*org0*].gov or [*orgN*.]…[*org0*].mil will be used to determine DNs. The first domain component of the DN will either be dc=gov or dc=mil. At least, the *org0* domain component must appear in the DN. The *org1* to *orgN* domain components appear, in order, when applicable and are used to specify the federal entity that employs the subscriber.

The distinguished name of the federal employee subscriber may take one of the three following forms when their agency's Internet domain name ends in .gov:

- dc=gov, dc=*org0*, [dc=*org1*], …[dc=*orgN*], [ou=*structural_container*], cn=*nickname lastname*
- dc=gov, dc=*org0*, [dc=*org1*],…[dc=*orgN*], [ou=*structural_container*], cn=*firstname initial. lastname*
- dc=gov, dc=*org0*, [dc=*org1*],…[dc=*orgN*], [ou=*structural_container*], cn=*firstname middlename lastname*

The distinguished name of the federal contractors and affiliated subscribers may take one of the three following forms when the agency's Internet domain name ends in .gov:

- dc=gov, dc=*org0*, [dc=*org1*],…[dc=*orgN*], [ou=*structural_container*], cn=*nickname lastname* (affiliate)
- dc=gov, dc=*org0*, [dc=*org1*],…[dc=*orgN*], [ou=*structural_container*], cn=*firstname initial. lastname* (affiliate)
- dc=gov, dc=*org0*, [dc=*org1*],…[dc=*orgN*], [ou=*structural_container*], cn=*firstname middlename lastname* (affiliate)

The distinguished name of the federal employee subscriber may take one of the three following forms when their agency's Internet domain name ends in .mil:

- dc=mil, dc=*org0*, [dc=*org1*], …[dc=*orgN*], [ou=*structural_container*], cn=*nickname lastname*
- dc=mil, dc=*org0*, [dc=*org1*],…[dc=*orgN*], [ou=*structural_container*], cn=*firstname initial. lastname*
- dc=mil, dc=*org0*, [dc=*org1*],…[dc=*orgN*], [ou=*structural_container*], cn=*firstname middlename lastname*

The distinguished name of the federal contractors and affiliated subscribers may take one of the three following forms when the agency's Internet domain name ends in .mil:

- dc=mil, dc=*org0*, [dc=*org1*],…[dc=*orgN*], [ou=*structural_container*], cn=*nickname lastname* (affiliate)
- dc=mil, dc=*org0*, [dc=*org1*],…[dc=*orgN*], [ou=*structural_container*], cn=*firstname initial. lastname* (affiliate)
- dc=mil, dc=*org0*, [dc=*org1*],…[dc=*orgN*], [ou=*structural_container*], cn=*firstname middlename lastname* (affiliate)

The CA may supplement any of the name forms for users specified in this section by including a dnQualifier, serial number, or user id attribute. When any of these attributes are included, they may appear as part of a multi-valued RDN with the common name or as a distinct attribute. Generational qualifiers may optionally be included in common name attributes in distinguished names based on Internet domain names. For names assigned to employees, generational qualifiers may be appended to the common name. For names assigned to federal contractors and other affiliated persons, generational qualifiers may be inserted between *lastname* and "(affiliate)".

Devices that are the subject of certificates issued under this policy may be assigned either a geo-political name or an Internet domain component name. Device names may take the following forms:

- C=US, o=U.S. Government, [ou=department], [ou=agency], [ou=*structural_container*], cn=*device name*
- dc=gov, dc=*org0*, [*dc=org1*], …[dc=*orgN*], [ou=*structural_container*], [cn=*device name*]
- dc=mil, dc=*org0*, [*dc=org1*], …[dc=*orgN*], [ou=*structural_container*], [cn=*device name*]

where *device name* is a descriptive name for the device. Where a device is fully described by the Internet domain name, the common name attribute is optional.

This policy does not restrict the directory information tree for names of CAs. However, CAs that issue certificates under this policy must have distinguished names. CA distinguished names may be either a geo-political name or an Internet domain component name.

CA geo-political distinguished names may be composed of any combination of the following attributes: country; organization; organizational unit; and common name. Internet domain component names are composed of the following attributes: domain component; organizational unit; and common name.

For certificates issued under id-fpki-common-authentication, assignment of X.500 distinguished names is optional. If assigned, distinguished names shall follow the rules specified above for id-fpki-common-hardware. Certificates issued under id-fpki-common-authentication shall include a subject alternative name. At a minimum, the subject alternative name extension shall include the pivFASC-N name type [FIPS 201]. The value for this name shall be the FASC-N [PACS] of the subject's PIV card.

Certificates issued under id-fpki-common-cardAuth shall include a subject alternative name extension that includes the pivFASC-N name type. The value for this name shall be the FASC-N of the subject's PIV card. Certificates issued under id-fpki-common-cardAuth shall not include any other name in the subject alternative name extension but may include a non-NULL name in the subject field. If included, the subject distinguished name shall take the following form:

- C=US, o=U.S. Government, [ou=*department*], [ou=*agency*], [ou=*structural_container*], serialNumber=*FASC-N*

Practice Note: The FASC-N [PACS] consists of 40 decimal digits that are encoded as a 25-byte binary value. This 25-byte binary value may be encoded directly into the pivFASC-N name type in the subject alternative name extension, but when included in the subject field the FASC-N must be encoded as a PrintableString that is at most 64 characters long. This policy does not mandate any particular method for encoding the FASC-N within the serial number attribute as long as the same encoding method is used for all certificates issued by a CA. Acceptable methods for encoding the FASC-N within the serial number attribute include encoding the 25-byte binary value as 50 bytes of ASCII HEX or encoding the 40 decimal digits as 40 bytes of ASCII decimal.

### 3.2.1 Certificate Renewal

Renewing a certificate means creating a new certificate with the same name, key, and other information as the old one, but with a new, extended validity period and a new serial number. Subscriber certificates issued under this policy shall not be renewed, except during recovery from CA key compromise (see 4.8.3). CA certificates and OCSP responder certificates may be renewed.

### 4.4.3 CRLs

CAs shall issue CRLs covering all unexpired certificates issued under this policy except for OCSP Responder certificates that include the id-pkix-ocsp-nocheck extension.

## 4.7 KEY CHANGEOVER

To minimize risk from compromise of a CA’s private signing key, that key may be changed often. From that time on, only the new key will be used for certificate signing purposes. If the old private key is used to sign OCSP responder certificates or CRLs that contain certificates signed with that key, the old key must be retained and protected.

The CA’s signing key shall have a validity period as described in Section 6.3.2.

### 6.3.2 Usage Periods for the Public and Private Keys

The usage period for the Common Policy Root CA key pair is a maximum of 20 years.

For all other CAs operating under this policy, t~~T~~he usage period for a CA key pair is a maximum of ~~six~~ ten years. The CA private key may be used to sign certificates for at most four years, but may be used to sign CRLs and OCSP Responder certificates for the entire usage period. All certificates signed by a specific CA key pair must expire before the end of that key pair’s usage period. ~~[Practice Note: For example, where subscriber certificates are issued with a three year lifetime, the CA private key may be used to generate certificates for the first half of the usage period (3 years), and the CA public key may be used to validate certificates for the entire usage period.] If the CA private key is used to sign CRLs, it may be used to sign CRLs for the entire usage period.~~

Subscriber public keys in certificates that assert the id-PIV-content-signing OID in the extended key usage extension have a maximum usage period of eight years. The private keys corresponding to the public keys in these certificates have a maximum usage period of three years.

All other s~~S~~ubscriber public keys have a maximum usage period of three years ~~one half the CA key pair usage period~~. Subscriber signature private keys have the same usage period as their corresponding public key. The usage period for subscriber key management private keys is not restricted.

**Estimated Cost:**

No cost.

**Implementation Date:**

This change will be implemented immediately upon approval by the FPKIPA and incorporation into the Common Policy CP.

**Prerequisites for Adoption:**

There are no prerequisites.

**Plan to Meet Prerequisites:**

There are no prerequisites.

**Approval and Coordination Dates:**

| | |
|---|---|
| Date presented to CPWG: | various throughout 2006 |
| Date Presented to FPKI PA: | 10 October 2006 |
| Date of approval by FPKI PA: | 10 October 2006 |